NATIONAL SECURITY AGENCY

OFFICE OF THE INSPECTOR GENERAL

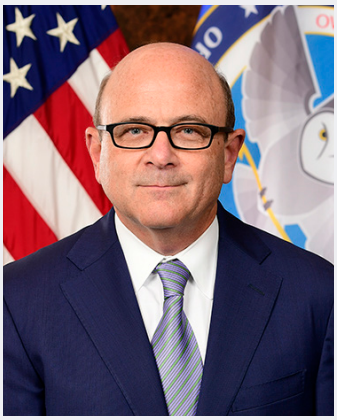
Semiannual Report to Congress

1 April to 30 September 2021

Pursuant to the Inspector General Act of 1978, as amended, and in accordance with NSA/CSS Policy 1-60, the NSA/CSS Office of the Inspector General (OIG) conducts independent oversight that promotes Agency respect for Constitutional rights, adherence to laws, rules, and regulations, and the wise use of public resources. Through investigations and reviews, we detect and deter waste, fraud, abuse, and misconduct and promote the economy, the efficiency, and the effectiveness of Agency operations.

NOTE: A classified version of the Semiannual Report (SAR) to Congress formed the basis of this unclassified version. The National Security Agency (NSA) Office of the Inspector General (OIG) has endeavored to make this unclassified version of the SAR as complete and transparent as possible. However, where appropriate, the NSA OIG has rephrased or redacted information to avoid disclosure of classified information and as required to protect NSA sources and methods and ensure the fairness and accuracy of the unclassified version of the report. In that regard, the classified version of this report contained descriptions of additional completed and ongoing work that could not be included in the public version of this report.

Message from the Inspector General



It is my pleasure and honor to submit the Semiannual Report for the National Security Agency (NSA) Office of the Inspector General (OIG) for the period ending 30 September 2021. During this reporting period, the team here at the OIG was remarkably productive, producing a total of 22 audits, inspections, evaluations, and other oversight products that make impactful findings and recommendations regarding a wide swath of this important Agency's work. Our Investigations Division continued to conduct and complete a number of significant investigations, addressing an increasing volume of contacts on both our classified and unclassified Hotlines. I believe this reflects a growing awareness within the workforce and beyond of the importance of reporting suspected wrongdoing to the OIG so that we can examine the circumstances and take such action as may be appropriate, and we will continue to work actively to encourage persons to come forward to provide our office with such critical information.

This is the eighth semiannual report that the OIG has issued since I came on board as the IG here, and I am pleased that it will be the eighth such report for which we prepare an unclassified version that we release publicly on our independent website, https://oig.nsa.gov, as well on the aggregator site for public reporting that is operated by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), https://www.oversight.gov. In addition to the unclassified versions or summaries of underlying oversight reports that we are able to prepare and release – including a significant report during this period on the OIG's *Audit of the NSA's Facilities and Logistics Service Contract* in which we questioned well over $400 million in costs – this substantial body of public reporting represents a major effort by the OIG to advance transparency to the greatest extent possible here.

Additionally, I would call the reader's attention to a new section in this semiannual report outlining the outstanding work of the OIG's Diversity and Engagement Committee (DEC). The DEC, which we set up shortly after I joined the OIG, conducts and coordinates a wide range of programming, training, and activities that reflect this office's commitment to diversity, equity, inclusion, and accessibility (DEI&A), and helps to ensure a full range of developmental opportunities for everyone on our team – all of which makes our work better and is, quite simply, the right thing to do for our people. We also are active participants in CIGIE's DE&I Work Group, which helps to share best practices and programming across the IG community in this critical area. I am truly pleased to showcase the important contributions of the DEC in the OIG's Semiannual Report for this period.

Finally, I would note that, with the end of the reporting period, my talented Deputy, Karen Butler, celebrated her well-deserved retirement after well over three decades of distinguished service to NSA and this office. We at the OIG benefited greatly from Karen's wisdom and her graciousness over the past several years, and we wish her every good wish as she moves into the next chapter of her life's journey.

Pursuant to the IG Act, I am pleased to report that the OIG experienced no attempts by the Agency to interfere with our independence and that the Agency fully cooperated with our work and did not refuse to provide or attempt to delay or restrict access to records or other information. Agency management agreed with all OIG recommendations that were made during the reporting period. All told, despite the continued difficult pandemic-related challenges facing many of our team during this reporting period, the OIG made a total of 469 recommendations to NSA leadership that we believe will be impactful in improving the economy, efficiency, and effectiveness of this critical Agency's operations.

ROBERT P. STORCH
Inspector General

Contents

OIG Executive Summary

Intelligence Oversight Division

The OIG's Intelligence Oversight (IO) Division issued two final reports during this period. One evaluation addressed whether NSA's Rules-Based Targeting (RBT) controls provide reasonable assurance that collection sites are selected for targeting efficiently, effectively, and in compliance with applicable authorities and directives. Our evaluation identified three primary areas of concern:

- NSA's targeting distribution process contained critical control gaps, in that it did not have adequate controls implemented to monitor the accuracy and completeness of the full targeting distribution process;
- Operational limitations, such as a lack of necessary site information, an insufficient number of personnel to consistently perform two-person validations, and the lack of a tool that would enable the Agency to systematically review all RBT configurations, hampered NSA's ability to effectively manage its RBT operations; and
- Data that NSA relied on to manage RBT rules was not efficiently, accurately, and completely maintained in Agency systems, which could cause targeting to be sent to the wrong sites.

Work At a Glance

Intelligence Oversight Division	**2**
Inspections Division	
Quick Reaction Reports	**1**
Inspections	**4**
Trends	**1**
Advisory Memoranda	**1**
Audits Division	**12**
Investigations Division	
Contacts	**700**
Closed Investigations	**32**
Closed Inquiries	**83**
Proposed Recoupment	**$71K**
Cases Referred to U.S. Attorney	**8**

As a result, we determined that NSA's RBT and targeting distribution deficiencies increase the likelihood both that NSA might inadvertently target selectors to locations that are prohibited by applicable NSA signals intelligence (SIGINT) collection authorities.

Another IO evaluation examined whether NSA analysts were appropriately documenting the foreign intelligence purpose and using approved U.S. person (USP) identifiers as query terms against Foreign Intelligence Surveillance Act (FISA) Section 702 data and in accordance with applicable query procedures. The evaluation revealed several issues that, if not addressed, have the potential to impact

the effectiveness of the Agency's internal controls used to protect the civil liberties and privacy rights of USPs. Specifically, as described in the Intelligence Oversight section of this report, the OIG's findings included that USP queries performed against FISA Section 702 data did not always follow NSA procedural and policy requirements, that some selector information within NSA's selector management tool was not documented with consistency, and that a NSA query tool did not prevent certain queries containing known USP selectors from processing.

Inspections Division

During this reporting period, the Inspections Division issued four inspection reports, one quick reaction report, and one advisory memorandum as well as a report of trends noted in OIG inspections performed over the last six calendar years.

As a result of the global COVID-19 pandemic, we performed one new inspection virtually and one inspection in a hybrid approach. In the latter situation, the OIG performed the majority of the inspection virtually and then sent two small teams to the site to assess areas that required in-person inspection. We have integrated the option to conduct physical, virtual, or hybrid inspections in our planning for future inspections.

The Cyberspace Workforce Improvement Program advisory memorandum highlighted the need for the Agency to formally identify a comprehensive list of work roles required to be certified in accordance with the Department of Defense (DoD) Information Assurance Workforce Improvement Program. The lack of work role identification formed a root cause for the repeat findings reported both across inspections and in audits.

Audits Division

The Audits Division is divided into three branches: Mission and Mission Support, Cybersecurity and Technology, and Financial Audits. The Audits Division had a productive reporting period, issuing 12 reports containing a total of 95 recommendations to improve Agency operations. Some of the highlights include the following:

The Mission and Mission Support branch performed various oversight efforts, including an audit of cost-reimbursement contracts. We found that the Agency was not performing sufficient review of actual costs on cost-reimbursement contracts. Noncompliance with contract clauses and insufficient billing documentation caused us to question labor charges of approximately $227 million and travel charges of over $226,000 – totaling approximately 75 percent of the costs in the invoices sampled. In addition, pursuant to a congressionally directed action, we issued an audit of NSA's Security & Counterintelligence focused on the effectiveness of NSA's posture against insider threats. We found internal oversight issues and deficiencies that increase the risks related to the identification of system vulnerabilities, physical and technical threats, and the introduction or removal of classified material.

The Mission and Mission Support branch also issued the *Audit of the Agency's Parking and Transportation Initiatives*. We found that the Agency had not identified parking as a priority, which led to Agency parking and transportation initiatives lacking sufficient goals, plans, and strategies. We also found that

the Agency's parking and transportation initiatives had significant internal control issues that resulted in the Agency wasting approximately $3.6 million dollars on a parking structure that had to be demolished without ever being used. Additionally, we issued the congressionally directed evaluation of *NSA's FY 2020 Application of Classification Markers, Compliance with Declassification Procedures, and the Effectiveness of Declassification Review Processes*. We found that classification authority blocks on finished reports did not comply with Executive Order (EO) 13526, Agency policy, or other Intelligence Community (IC) and DoD requirements.

The Financial Audits branch issued a *Quick Reaction Report (QRR) on Appropriations for Radome Purchases and Installations* in response to a hotline complaint. Although we found that the complainant's specific allegation was unsubstantiated, we found that depending on whether radomes were legally characterized as personal property (equipment) or real property (public buildings or improvements), NSA inappropriately funded either 1 or 14 radomes resulting in a potential Antideficiency Act (ADA) violation of approximately $451,000 or $8.7 million.

Investigations Division

During this reporting period, the Investigations Division received and processed 700 contacts on our classified systems, reflecting the continuation of an upward trend in contacts that resulted in the initiation of 32 new investigations and 83 new inquiries. Investigations include allegations into violations of standards of conduct, computer misuse, hostile work environment, contractor labor mischarging, travel card misuse, time and attendance fraud, government vehicle misuse, and reprisal. Forty-two investigations and 122 inquiries were closed during the reporting period, resulting in the proposed recoupment to the Agency of approximately $70,999 from employees and $681,688 from contractors. OIG investigations resulted in actual recoveries of $43,133 to the Government. As a result of OIG investigations, 21 employees retired, resigned in lieu of removal, or had other disciplinary actions taken ranging from termination to no action. Eighteen cases referred to the U.S. Attorney for the District of Maryland were declined for prosecution.

Significant Problems, Abuses, and Deficiencies and Other Particularly Significant Reports

OIG projects during the reporting period did not reveal serious or flagrant problems or abuses related to the administration of Agency programs or operations that would require immediate reporting to the Director, NSA (DIRNSA), and Congress pursuant to Section 5(d) of the Inspector General (IG) Act. However, the following reviews revealed significant problems, abuses, or deficiencies, or were otherwise particularly significant reports as provided in Section 5(a) of the Act:

Trends Noted in OIG Inspections August 2014-December 2020

During the 57 site inspections of NSA field elements carried out from August 2014 through December 2020, numerous issues identified by the OIG were found in multiple, if not all, locations inspected. Given the differing composition of sites inspected and the evolution of applicable policies and guidance, as well as the need for the OIG to adjust some inspections to focus on document review or to be conducted virtually as a result of the COVID-19 pandemic, not every site was evaluated in every area, which impacts the numbers reported for each category. Nevertheless, this report provided an overview of the most prominent repeat findings in each of the areas examined by the OIG – command topics, mission operations, intelligence oversight, resource programs, information technology and systems, safety and facilities, security, and training – to assist leaders across the Agency as they consider their own organizational processes, practices, and structure. This report also highlighted commendable practices to help organizations identify how others addressed similar findings with holistic solutions or mitigations to recurrence.

Quick Reaction Report on Concerns Discovered during an Inspection of the Cryptologic Services Group Key West

During its inspection of the Cryptologic Services Group Key West, the OIG discovered that a support group attached to a joint inter-agency task force was accessing data without the proper authorization. The OIG made five recommendations to assist the Agency in bringing the activity into compliance with governing authorities and policies.

Audit of Cost-Reimbursement Contracts

The overall objective of this audit was to determine whether the Agency has effective and efficient internal controls over cost-reimbursement contract expenses.

This audit revealed the following concerns involving cost-reimbursement contracts:

- The Contracting Officer Representative (COR) process was ineffective and inefficient. The OIG determined that the Agency had inadequate oversight of the actual costs of cost-reimbursement contracts due to vague and ineffective COR roles, responsibilities, and oversight procedures. Additionally, tools that did not meet the demands of managing large, complex cost-reimbursement contracts with voluminous Technical Task Orders (TTOs)

added to a heavy COR workload. The Agency's process for managing expenses on cost-reimbursement contracts did not fulfill its responsibility to mitigate the significant risks associated with these type of contracts.

- The Agency was not performing sufficient reviews of actual costs on cost-reimbursement contracts. This was due to contract clauses not being enforced, a lack of focus on actual costs with an overemphasis on tracking funding by TTO, an overreliance on contractor-provided reports, and no risk assessment for high-risk contractors. Noncompliance with contract clauses and insufficient billing documentation caused the OIG to question labor charges of approximately $227 million and travel charges of over $226,000 – totaling approximately 75 percent of the costs in the invoices sampled.
- There was limited external oversight of actual costs for cost-reimbursement contract expenses due to inadequate and unmanaged communication with the Defense Contract Audit Agency (DCAA), as well as a lack of understanding regarding contract auditors' coverage of Agency contracts. As a result, the Agency has increased risk of further labor mischarging and of making improper payments for unallowable costs.

The findings identified by the OIG in this audit highlight the increased risks of payments for unallowable costs and further labor mischarges. These deficiencies have the potential to impact the proper determination as to whether cost-reimbursement contract costs are allowable, allocable, and reasonable. Additionally, cost-reimbursement contract costs could go without examination by an Agency contracting official, such as a COR, or by external auditors. Failure to review actual costs and limited external oversight increase the risk of improper billings and payments in cost-reimbursement contracts.

The OIG made 22 recommendations to assist the Agency in addressing the significant issues in this report.

Audit of Network Enclaves with Distributed Monitoring Oversight

The overall objective of the audit was to determine whether Agency network enclaves with distributed monitoring oversight were secured in accordance with Agency, DoD, and federal policies. The OIG conducted an assessment of information security controls for a sample of network enclaves and associated systems. The OIG made 12 recommendations to assist the Agency in addressing the findings of the report. The actions planned by management meet the intent of all recommendations.

Congressionally Required Audit on NSA's Security & Counterintelligence

The OIG conducted this audit on NSA's Security and Counterintelligence (S&CI) pursuant to a congressional mandate. This mandate directed the OIG to focus the audit on the effectiveness of NSA's posture against insider threats with an emphasis on how NSA has organized S&CI, the activities undertaken by S&CI, and the effectiveness of S&CI programs and initiatives associated with mitigating insider threats.

This audit revealed that S&CI has five offices that support the Insider Threat Program (ITP). These offices and resources supported 22 direct and 5 indirect insider threat activities. Upon review of selected insider threat activities, we identified concerns related to the effectiveness of the programs and initiatives used by S&CI to mitigate potential insider threats. While these findings cannot be detailed

in a public report, we found that there was an increase in risks related to the identification of system vulnerabilities, physical and technical threats, and the introduction or removal of classified material. Additionally, the OIG found that S&CI could not account for 46 percent of the confiscation forms, which contain personally identifiable information (PII), that were confiscated from NSA visitors and affiliates. This occurred because these forms were created in hard-copy format and passed through multiple organizations. The OIG made 15 recommendations—one of which was closed prior to issuance of the report—to assist the Agency in addressing these important issues.

Quick Reaction Report on Appropriations for Radome Purchases and Installations

The NSA OIG hotline received a complaint alleging that the Agency improperly used procurement appropriations to fund the installation of radomes at an overseas site. Although we found that the complainant's specific allegation was unsubstantiated, we identified other issues during our review. We found that depending on whether radomes were legally characterized as personal property (equipment) or real property (public buildings or improvements), NSA inappropriately funded either 1 or 14 radomes resulting in a potential Antideficiency Act (ADA) violation of approximately $451,000 or $8.7 million. NSA may have incurred an ADA violation(s) of the purpose statute, which requires that appropriations be used only for the object for which they were intended, based upon its characterization of the end item it was acquiring and its apparent failure to identify the correct appropriation accordingly.

Additionally, we found that NSA improperly purchased radomes without identifying the funds to install them, which violates the Office of Management and Budget (OMB) and DoD full funding policies. The full funding policy is intended, in part, to prevent the completion of a project from being dependent on future appropriations. Because of a lack of planning and dedicated funding to move and install the radomes, NSA had to purchase two years of additional storage at a cost of approximately $10,800.

The OIG issued a QRR because we identified matters that we believe warranted the Agency's prompt attention and because the potentially impacted appropriations cancel on 30 September 2021. Under either potential ADA scenario, the Agency could cure the potential ADA if it had funds available in the correct appropriation and the proper funds were available at the time of the original obligation. The OIG made three recommendations to assist the Agency in addressing the issues identified in the QRR, and the Agency agreed with all the recommendations.

Summary of Reports for Which No Management Decision Was Made

No reports without management decisions were published.

Significant Revised Management Decisions

There were no significant revised management decisions regarding OIG reports.

Significant Management Decision Disagreements

There were no significant management decisions with which the OIG was in disagreement regarding OIG reports.

Intelligence Oversight

Evaluations and Oversight Memoranda Completed in the Reporting Period

Evaluation of NSA's Rules-Based Targeting Controls

Rules-Based Targeting (RBT) refers to a NSA targeting tool's method of automating site selections when targeting a given selector. The OIG conducted this evaluation to determine whether NSA's RBT controls provide reasonable assurance that collection sites are selected for targeting efficiently, effectively, and in a manner that complies with NSA's SIGINT collection authorities and policy.

The evaluation revealed the following concerns:

- NSA's targeting distribution process contained critical control gaps.
- NSA did not have a system control to provide reasonable assurance that essential data in a supporting system and NSA's targeting tool was accurately aligned prior to the tool initiating the targeting distribution process. NSA did not have sufficient controls to provide reasonable assurance that approved targeting packages were made available only to the correct U.S. Government-controlled collection sensors.
- Operational limitations hampered NSA's ability to effectively manage RBT operations.
- NSA's ability to effectively manage RBT controls was hampered by several factors, including a lack of necessary site information, an insufficient number of personnel to consistently perform two-person validations, and the lack of a tool that would enable the Agency to systematically review all RBT configurations.
- Data that NSA relied on to manage RBT rules was not efficiently, accurately, and completely maintained in Agency systems.
- NSA relied on similar systems with incomplete information to obtain data and execute certain processes needed to manage NSA's RBT controls. The OIG further found that site information maintained in existing systems was not always accurate and complete.

The OIG made 17 recommendations to assist NSA in addressing these issues.

Evaluation of United States Person Identifiers Used to Query FISA Section 702 Data

The OIG conducted this evaluation to assess the effectiveness of the internal controls used to protect USP privacy rights by determining whether NSA analysts were appropriately documenting the foreign intelligence purpose and using approved USP identifiers as query terms against FISA Section 702 data and in accordance with FISA Section 702 query procedures.

The evaluation revealed a number of concerns involving USP identifiers used as query terms against FISA Section 702 data, including:

- **USP queries performed against FISA Section 702 data did not always follow NSA procedural and policy requirements.**

  Queries performed using USP selectors in FISA Section 702-acquired content and metadata did not always follow Foreign Intelligence Surveillance Court (FISC)-approved NSA query procedures and NSA internal policy requirements. While NSA has implemented both preventative and detective controls, the Agency has not completed the development of a preventative system control that performs pre-query validation to notify analysts of potential noncompliance with NSA query procedures or policy problems prior to query execution.

- **Some selector information in an NSA tool's FISA Section 702 USP query module was not documented with consistency.**

  NSA's tool provides a single access point for selector management, supporting various NSA authorities for both compliance and operational requirements. Some selector information was not documented in a consistent format in the tool's FISA Section 702 USP query module. The lack of consistency limited the ability to fully and accurately search the module's contents. Furthermore, data standards were not fully addressed in NSA's tool, and the tool lacked standard operating procedures that were accessible to analysts with access to the tool.

- **An NSA query tool did not prevent certain queries containing known USP selectors from processing.**

  An NSA query tool's internal controls did not include measures to prevent queries of known USP selectors from executing automated follow-on queries if the query term was not included on the tool's defeat list.

The OIG made 13 recommendations to assist NSA in addressing these issues. Seven recommendations were closed prior to report issuance, and the actions planned by management meet the intent of the other recommendations.

Ongoing Intelligence Oversight Work

Special Study of the Process to Purge Signals Intelligence Data from NSA Source Systems of Record

The objective of this review is to assess the effectiveness and efficiency of NSA's process to find, and quarantine or remove, unauthorized or otherwise noncompliant SIGINT data completely, reliably, and in a timely manner in accordance with legal and policy requirements.

Limited-Scope Evaluation of Mission Correlation Table Data

The objective of this evaluation is to test the effectiveness of controls for Mission Correlation Table (MCT) data, including, for example, assigning mission authorities, location, and members to an MCT; managing MCT and mission member entitlements; granting mission members access to SIGINT data in NSA repositories; and administering MCT roles and responsibilities.

Inspectors General of the IC and NSA Joint Review of Management and Intelligence Oversight at the Intelligence Community Advanced Campaign Cell (ACC)

The objective of this joint review by the IGs of the IC and NSA is to determine whether management and intelligence oversight of the IC ACC ensures that processes and procedures are in place to conduct operations that comply with IC and DoD policies. The joint review will present any issues to the Director of National Intelligence and DIRNSA for resolution, as appropriate.

Evaluation of the Procedures for Continental U.S. (CONUS) Wireless Signals Testing and Training

The objective of this evaluation is to determine the effectiveness and efficiency of procedures for conducting wireless signals collection testing and training in CONUS non-sensitive compartmented information facility areas and the degree to which those procedures ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of a Targeting System's Control Framework for Domestic and Foreign Partner Targeting Systems

The objective of this evaluation is to determine the effectiveness and efficiency of a targeting system's control framework as it relates to domestic and foreign partner targeting systems, with emphasis on NSA's handling of partner targeting requests. The evaluation will also examine how NSA prepares some targeting requests prior to sending them to partner targeting systems, as well as evaluate the targeting system's internal controls and the degree to which those controls ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of NSA's LEGALEAGLE System Enrollment, Data Ingest, and Decision-Logic Processes

The objectives of this evaluation are to determine the effectiveness of NSA's process for identifying and registering systems, ensuring the integrity of ingested records, validating the decision-logic processes, and validating the effectiveness of LEGALEAGLE's operations and associated controls in ensuring compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of NSA's Implementation of Title I FISA Authority

The objective of this evaluation is to assess the efficiency and effectiveness of the Agency's implementation of Title I FISA authority, to include evaluating compliance with the applicable targeting and minimization procedures as well as the efficiency and effectiveness of the controls designed to reasonably ensure the protection of individual civil liberties and privacy rights.

Evaluation Related to Alleged NSA Targeting of a Member of the U.S. Media

This review relates to recent allegations that NSA improperly targeted the communications of a member of the U.S. news media. The OIG is examining NSA's compliance with applicable legal authorities and Agency policies and procedures regarding collection, analysis, reporting, and dissemination

activities, including unmasking procedures, and whether any such actions were based on improper considerations. If circumstances warrant, the OIG will consider other issues that may arise during the review.

Joint Department of Homeland Security (DHS)/NSA OIG Evaluation of Cyber Intrusion Prevention Efforts

The objective of this joint evaluation is to assess the actions taken by NSA and DHS in advance of, or in connection with, recent intrusions into USG and private sector networks. The evaluation team will use the SolarWinds Orion and related intrusions as use cases to identify relevant authorities NSA and DHS used and determine if the agencies executed activities in accordance with those authorities. The team will also assess the efficacy of the policies, procedures, and mechanisms used to address threats and share information with appropriate stakeholders.

INSPECTIONS

Inspection Reports and Oversight Memoranda Completed in the Reporting Period

Inspection of the NSA/CSS Representative and Cryptologic Services Group to U.S. European Command (NCR EUCOM)

The OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NSA/CSS Representative (NCR) and Cryptologic Services Group (CSG) to U.S. European Command (EUCOM) during an inspection. During the inspection, the OIG interviewed members of the NCR and CSG EUCOM (collectively referred to herein as "NCR EUCOM") workforce and observed operations and functions in the areas of command topics; mission operations; intelligence oversight; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training. NCR EUCOM leadership and personnel fully supported the OIG during this inspection.

We found that the morale and quality of life for personnel at NCR EUCOM were generally good. However, we noted that personnel would benefit from more consistent messaging from leadership, particularly in light of the anticipated move to a new facility and the possibility of an organizational restructure.

The OIG identified a number of concerns at NCR EUCOM, including safety concerns related to the aging site facilities. In addition, the OIG noted outdated, incomplete, or missing documentation across several functional areas, including an out-of-date and incomplete continuity of operations plan; the lack of designated records management officers; and several issues related to information system security, including concerns about data center management.

The OIG made 61 recommendations (including one carried forward from the previous inspection) and 6 observations to assist NCR EUCOM and the Agency in addressing the findings identified during the inspection. In addition, the OIG noted two commendable practices in the areas of security and training.

Inspection of the NSA/CSS Representative and Cryptologic Services Group to U.S. Africa Command (NCR AFRICOM)

The OIG evaluated the overall climate, compliance with laws and policies, and the efficiency and effectiveness of the activities of the NCR and CSG to U.S. Africa Command (AFRICOM) during an inspection. During the inspection, the OIG interviewed members of the NCR and CSG AFRICOM (collectively referred to herein as "NCR AFRICOM") workforce and observed operations and functions in the areas of command topics; mission operations; intelligence oversight; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training. NCR AFRICOM leadership and personnel fully supported the OIG during this inspection.

Overall, we found that morale and quality of life among site personnel was generally good, and site members praised the leadership and support of the NCR at the time of the inspection. As at NCR EUCOM, the OIG noted that personnel would benefit from more consistent messaging from leadership.

The OIG identified a number of concerns at NCR AFRICOM, including safety issues related to the aging site facilities. In addition, the OIG noted outdated, incomplete, or missing documentation across several functional areas, including the lack of designated records management officers and a number of information system security concerns.

The OIG made 57 recommendations (including 4 carried forward from the previous inspection) and 5 observations to assist NCR AFRICOM and the Agency in addressing the findings identified during the inspection. In addition, the OIG noted two commendable practices in the areas of security and training.

Cyberspace Workforce Improvement Program—Advisory Memorandum

NSA/CSS Policy 6-34, *NSA/CSS Cyberspace Workforce Improvement Program*, issued 21 December 2015, establishes a training and certification program that provides cyberspace professionals with a common set of information assurance/cyber skills and knowledge. The policy, which implements DoD Directive 8140.01, *Cyberspace Workforce Management*, issued 11 August 2015, and DoD 8570.01M, *Information Assurance Workforce Improvement Program*, issued 10 November 2015, specifies that managers, contracting officers, and CORs are responsible for identifying all positions that are required to perform information assurance and cyberspace (IA/CYBER) functions. The NSA Cyberspace Workforce Improvement Program (CWIP) office was established to support NSA in identifying and tracking IA/CYBER billets and positions.

Based on observations from multiple inspections, the OIG has determined that many Agency affiliates assigned to perform cyberspace work have not met the CWIP qualification standards required for those roles. The OIG has frequently heard in interviews and focus groups that personnel were unaware of the requirements, decisions had not been made to specify which personnel or billets were required to attain certification, and personnel did not have the opportunities or resources to obtain required training and certification to become fully qualified. The OIG has determined that the Agency lacks a robust process for identifying affiliates working in cyberspace roles.

The OIG made three recommendations to assist the Agency in identifying all NSA affiliates who perform IA/CYBER functions on Agency system security plans, to determine which IA/CYBER functions require CWIP certification, and to identify and notify all personnel who perform IA/CYBER functions of their responsibilities and the expectations for their completion of CWIP certification. The Agency agreed with all three recommendations.

Short-Notice Inspection of NSA/CSS Representative to Defense Information Systems Agency/Joint Force Headquarters—Department of Defense Information Network

The NSA OIG inspection team conducted a short-notice inspection to evaluate the overall climate and the efficiency, effectiveness, and compliance of the NCR to Defense Information Systems Agency/Deputy NCR, U.S. Cyber Command for Joint Force Headquarters-Department of Defense Information Network (NCR DISA).

The OIG interviewed members of the NCR DISA management and workforce with regard to NCR DISA's operations and functions in the areas of command topics; mission operations; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training. NCR leadership and personnel supported the OIG throughout this inspection. Overall, we found site personnel were encouraged by the communications with the site's most senior leader. We identified several best practices and a number of concerns, the latter of which include the following:

- **Command topics**: The support provided by the NCR team received glowing praise from DISA and the joint force headquarters leaders. However, the inspection identified concerns regarding a need to confirm and document the full responsibilities of the NCR and to assess and document the resources needed to carry out the NCR's mission.
- **Mission operations**: Concerns identified in this inspection area included incomplete mission documentation, a potential gap with respect to critical information (CRITIC) reporting and training requirements, and a lack of documentation supporting knowledge transfer.
- **Resource programs**: Within this inspection area, the OIG identified concerns related to support agreements, records management, personnel acknowledging the nepotism statement, and NSA visitors to NCR DISA's area of responsibility.
- **Information technology and systems**: The OIG had no significant negative findings with regard to the NCR DISA information technology and systems.
- **Safety, facilities, and emergency management**: Within this inspection area, the OIG identified concerns related to safety, facilities, and emergency management.
- **Training**: Within this inspection area, the OIG identified concerns related to mandatory training and professional development.

The OIG made 36 recommendations, including 1 recommendation carried forward from a previous OIG inspection on a matter we also saw at NCR DISA, and 4 observations to assist the site in addressing the findings identified during the inspection.

Joint Inspection of an Overseas Site

The NSA, Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 25th Air Force OIGs jointly conducted an inspection that evaluated the overall climate, compliance with laws and policies, and efficiency and effectiveness of the programs and operations of an overseas site. During the inspection, the joint inspection team conducted focus groups, participants of which represented

all segments of the civilian and military government workforce. The OIG also interviewed members of the workforce and observed operations and functions in command topics; mission operations; intelligence oversight; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training.

Overall, we found site personnel were encouraged by the communications with the site's most senior leader. We identified several best practices and a number of concerns, including the following:

- **Command topics**: The OIG noted key areas of concern including the lack of a consistent approach to keeping the workforce informed, a lack of strategic direction, and a need for a thorough review and analysis of staffing.
- **Mission operations**: The OIG identified concerns in the areas of incomplete mission documentation; noncompliance with training requirements for handling sensitive material; the lack of a defined analytic integrity standards program; shortfalls in mission integration; noncompliance with the CRITIC test and evaluation program requirements; and a lack of reliable and robust tools supporting analytic missions.
- **Intelligence oversight**: The OIG assessed the site's intelligence oversight program as adequate but in need of improvement, primarily concerning documentation, awareness, training, and the overall climate of complacency of the workforce with regard to intelligence oversight.
- **Resource programs**: The OIG identified concerns in various personnel programs, the protection of site visitors' PII, support and partnership agreements, property accountability, and records management.
- **Safety, facilities, and emergency management**: The OIG identified concerns related to safety, facilities, and emergency management.
- **Training**: The OIG found that not all personnel had completed mandatory training and noted deficiencies in operations training and professional development.

The OIG made a total of 188 recommendations, including 1 recommendation that was carried forward from a previous OIG special study, and 4 observations to assist the site and the Agency in addressing the findings identified during the inspection. In addition, the OIG noted one commendable practice that we believe may warrant replication elsewhere across the NSA enterprise.

Ongoing Inspections Work

During the current reporting period, the Inspections Division continued to work on the following evaluations:

Assessment of NSA's Personnel Accountability Program

DoD Instruction (DoDI) 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, issued 3 May 2010, establishes policy and assigns responsibilities for accounting and reporting of DoD-affiliated personnel following a natural or man-made disaster. Since CY 2011, DoDI 3001.02 has required the IGs of the DoD components to conduct evaluations biennially of the personnel accountability programs in their respective components to ensure compliance with this instruction. This is the OIG's sixth biennial evaluation of NSA's personnel accountability program.

Evaluation of Mission Assurance/Continuity of Operations

The OIG has noted Continuity of Operations program concerns across the last several years of inspections and has cited this topic in the Semiannual Report to Congress as a significant outstanding recommendation to elevate the importance for the Agency to address the continuing challenge. The COVID-19 pandemic has reinforced the need to evaluate the effectiveness and efficiency of NSA's Mission Assurance/Continuity of Operations program and to determine whether the program meets all of the requirements of pertinent policies and regulations.

In addition to the above, the OIG continues to work on reports for five inspections that evaluated the overall climate and the compliance, effectiveness, and efficiency of the following organizations:

- Inspection of NSA/CSS Representative and Cryptologic Services Group to U.S. Southern Command and Cryptologic Services Group Key West;
- Inspection of NSA/CSS Representative and Cryptologic Engagement Group to U.S. Central Command;
- Inspection of NSA/CSS Representative and Cryptologic Services Group to U.S. Special Operations Command;
- Inspection of NSA/CSS Representative and Cryptologic Services Group to North American Aerospace Defense Command/U.S. Northern Command; and
- Inspection of NSA-Utah.

AUDITS

Audit Reports and Oversight Memoranda Completed in the Reporting Period

Audit of NSA's Fiscal Year 2020 Compliance with the Payment Integrity Information Act of 2019

The OIG *Audit of NSA's Fiscal Year 2020 Compliance with the Payment Integrity Information Act of 2019* (PIIA) determined that NSA is in compliance with PIIA. Using the procedures outlined in the Office of Management and Budget (OMB) Circular A-123, Appendix C, "Requirements for Payment Integrity Improvement," 26 June 2018, the OIG found that the Agency complied with all six statutorily required improper payment reporting requirements for the fiscal year that ended on 30 September 2020. The OIG did make one recommendation to assist the Agency in improving regular pay testing to prevent future improper payments.

Audit of the Agency's Parking and Transportation Initiatives

The overall objective of this audit was to assess the economy, efficiency, and effectiveness of recent parking and transportation initiatives, and to determine if they were in compliance with applicable laws, regulations, policies, and best practices.

For decades, Agency employees have expressed concerns about parking at NSA Washington (and specifically at the Big Four buildings on Fort Meade). However, the Agency has not identified parking as a priority and has failed to successfully implement solutions that would minimize the shortage, which has resulted in poor employee morale. Due to lack of prioritization by the Agency, the OIG found the following concerns:

- Agency parking and transportation initiatives lacked sufficient goals, plans, and strategies. Without established goals, plans, or strategies, the Agency cannot effectively plan for future initiatives.
- Agency parking and transportation initiatives had significant internal control deficiencies, such as the lack of a consistent process for developing, approving, and implementing parking and transportation initiatives. This resulted in the Agency wasting approximately $3.6 million dollars on a parking structure that had to be demolished without ever being used.
- The overall monitoring and administration of parking at the Agency is lacking processes and procedures. For example, the reserved parking permits have been over distributed and not effectively managed or enforced. Additionally, the database for tracking registered vehicles was outdated and incomplete, making it unreliable and unusable for its intended purpose. These inefficiencies make it difficult for employees to find appropriate parking and for the Agency to accurately plan and adjust spaces as needed.

- The Agency's system for reserving government vehicles needs improvement. Agency employees can reserve a government vehicle without a clear understanding of the policy, which can lead to misuse by Agency employees.

The findings identified by the OIG in this audit highlight the lack of centralized strategic planning, poor initiative implementation, and ineffective monitoring that has created control deficiencies and wasted funds and has negatively impacted employee morale. The OIG made 6 findings and 16 recommendations to assist the Agency in addressing these issues.

Appropriations for Radome Purchases and Installations, Quick Reaction Report

See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Audit of the Agency's Management of Fit-up Costs

The original objective of the audit was to assess the economy and effectiveness of NSA's fit-up process and to determine whether shared operating expenses were properly allocated to other agencies occupying NSA buildings. However, we determined that the fit-up and shared operating expenses processes were not closely related; therefore, we addressed each process separately. The allocation of shared expenses is addressed below in the *Audit of the Allocation of Shared Expenses*. The objective of this audit was to assess the economy and effectiveness of NSA's fit-up process. "Fit-up" is the Agency's term for making interior office spaces suitable for mission operations.

The OIG assessed that Installations & Logistics (I&L) could not effectively manage fit-up projects because it lacks necessary information from enabling organizations and processes. As a result, the Agency cannot track the total cost of fit-up projects to determine if funds are spent appropriately, which could impact the budgeting process and the Agency's financial statements. The OIG made one recommendation to assist the Agency with the issues identified in the report and found that management's planned actions met the intent of that recommendation.

Audit of Cost-Reimbursement Contracts

See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Evaluation of the NSA Information Security Continuous Monitoring Program

The objective of the review was to evaluate NSA's Information Security Continuous Monitoring (ISCM) Program based on information obtained during the FY 2020 Federal Information Security Modernization Act (FISMA) evaluation. The results of this evaluation will be incorporated in an Intelligence Community Inspector General (ICIG) capstone report summarizing IC-wide ISCM maturity.

Our assessment highlights findings previously reported in the OIG's FY 2020 FISMA evaluation. According to that evaluation report, the ISCM Program was designated at a maturity level of

"Defined," which indicates that it is not consistently implemented. Previous OIG FISMA evaluations have noted recurring areas for improvement in the Agency's ISCM Program. However, NSA has drafted a strategic plan for the ISCM Program, but it does not specifically address how the program will evolve to meet the maturity level requirements for level 3 or level 4. The Agency asserted that it has made progress in a number of areas that the OIG anticipates assessing in connection with the FY 2021 FISMA evaluation. There are no new recommendations for action in this report.

Audit of the Allocation of Shared Expenses

The objective of this audit was to determine whether shared operating expenses were properly allocated to other agencies occupying NSA buildings. NSA has relationships with other government agencies, which sometimes require tenancy, along with facilities and logistics services, at the Agency. Non-NSA organizations that occupy space at the Agency are considered non-Agency tenants.

The OIG found the Agency is not properly managing non-Agency tenant agreements and costs concerning NSA spaces. There is no process to ensure that appropriate support agreements are in place prior to allocating space to such non-Agency tenants. Additionally, the data used to track non-Agency tenants and to calculate the per-seat fees charged to U.S. Cyber Command are out of date and inaccurate. As a result, there could be substantial risk that the Agency is improperly absorbing costs associated with non-Agency tenants.

The OIG made three recommendations to assist the Agency in addressing this finding

Audit of Network Enclaves with Distributed Monitoring Oversight

See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Evaluation of NSA's FY 2020 Application of Classification Markers, Compliance With Declassification Procedures, and the Effectiveness of Declassification Review Processes

Section 6721 of the National Defense Authorization Act for FY 2020 (Public Law 116-92, issued 20 December 2019) directed IC OIGs to submit a classification review report to the congressional intelligence committees. Pursuant to this congressional directive, the overall objective of the evaluation was to analyze the following with respect to FY 2020:

- The accuracy of the application of classification and handling markers on a representative sample of finished reports, including such reports that are compartmented;
- Compliance with declassification procedures; and
- The effectiveness of processes for identifying topics of public or historical importance that merit prioritization for a declassification review.

The OIG found that classification authority blocks on finished reports did not comply with EO 13526, NSA/CSS Policy Manual 1-52, or other IC and DoD requirements. This was due to flawed reporting tools, lack of classification knowledge, insufficient report review (including an incomplete self-inspection assessment), and outdated classification guides. This evaluation also revealed that NSA's Declassification Services did not complete all mandatory declassification review

requests within specified timeframes. Specifically, final determinations on the review requests were not made within one year from the date of receipt, which is not compliant with the Code of Federal Regulations. These delays occurred because of COVID-19 restrictions and a lack of effective controls.

The findings identified by the OIG in this evaluation revealed that the Agency cannot ensure that classified information is protected and shared at the correct level. Further, transparency may be limited as a result, potentially impacting otherwise appropriate public access to information about Agency activities. The OIG made 13 recommendations in the report, and the actions planned by management met the intent of all recommendations.

Congressionally Required Audit on NSA's Security & Counterintelligence

See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Audit of Tactical Serialized Reporting

NSA uses a variety of serialized reporting vehicles to convey SIGINT information to customers throughout the IC. A tactical serialized report (TGRAM) is one of the serialized reporting vehicles that can be used to disseminate SIGINT in support of tactical operations.

This audit revealed the following concerns involving TGRAMs:

- A significant portion of the 30 TGRAM reports examined by the OIG were not compliant with reporting guidance. The OIG believes this was because NSA authors and releasers of TGRAMs were not provided with TGRAM-specific training and because of a lack of enforcement of existing SIGINT reporting training requirements. After our review of the TGRAM reports in this audit, the Agency implemented a TGRAM-specific training course, but the course is not readily available to all of those who need it. Until the Agency improves compliance with reporting guidance, Agency information may be improperly shared.
- The Agency did not effectively manage who had access to reports with restricted access. Without effective management over the program, affiliates without a need to know will have unauthorized access to restricted intelligence, which could increase the risk that reports are improperly shared.

The OIG made nine recommendations to assist the Agency in addressing these issues.

FY 2021 Statement of Standards for Attestation Engagement 18, NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

We contracted with an independent public accounting firm to perform an examination of NSA's description of its system supporting the performance of financial processing services on behalf of another U.S. Government organization from 1 October 2020 through 30 June 2021, and the suitability of the design and the operating effectiveness of controls to achieve the related control objectives stated in the description. The examination noted certain exceptions, including with the description of a system and the design, implementation, and operating effectiveness of controls, which resulted in a qualified opinion.

Ongoing Audit Work

Audit of the Implementation of the Coronavirus Aid, Relief, and Economic Security (CARES) Act, Section 3610

In this audit, the OIG will determine whether NSA has economically, effectively, and efficiently implemented Section 3610 of the CARES Act with regard to payments made to Agency contractors.

Audit of the FY 2021 National Security Agency Financial Statements

The purpose of this audit is to express an opinion on whether the financial statements are presented fairly and in conformity with U.S. generally accepted accounting principles. The audit will consider and report on internal control over financial reporting and compliance with certain laws, regulation, and other matters.

Evaluation of the NSA/CSS Implementation of the Federal Information Security Modernization Act of 2014 (FISMA)

The overall objective of this evaluation will be to review the Agency's information security program and practices. In accordance with OMB guidance, we will assess the overall effectiveness of the Agency's information security policies, procedures, and practices.

Oversight Review of the NSA Restaurant Fund and the NSA Civilian Welfare Fund

The overall objective of this oversight review is to ensure that the audits performed by an independent public accounting firm of the financial statements of the NSA Restaurant Fund and the NSA Civilian Welfare Fund as of and for the fiscal years that ended 30 September 2020 and 2019 were performed in accordance with generally accepted U.S. government auditing standards and the terms of the contract for non-appropriated fund instrumentalities audit services.

Joint Evaluation of the National Security Agency Integration of Artificial Intelligence

The overall objective of the evaluation is to assess NSA's integration of artificial intelligence into SIGINT operations in accordance with DoD and IC guidance for artificial intelligence.

INVESTIGATIONS

Criminal Prosecutions

The OIG continues to provide support for ongoing criminal cases the OIG referred to the Department of Justice (DOJ).

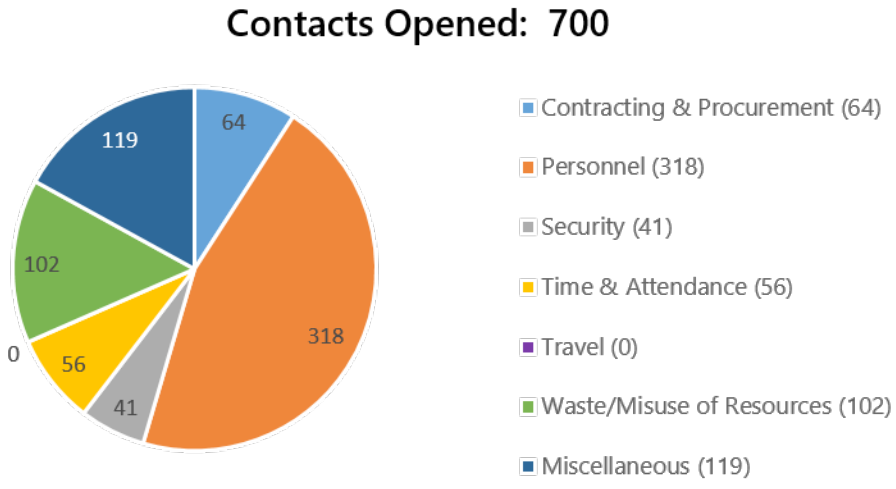
OIG Referrals

In accordance with section 4(d) of the IG Act and 5 U.S.C. appendix, the Investigations Division reported 18 cases to DOJ during the reporting period. In each case, the OIG had reasonable grounds to believe that a violation of federal criminal law had occurred. The allegations referred included activity such as contractors submitting false labor charges. The OIG anticipates at this time that the Government is likely to handle these cases administratively rather than criminally.

The Investigations Division referred 22 new cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the Agency notified the OIG of disciplinary decisions for 21 employees based on OIG reports. Six employees retired or resigned in lieu of removal, two employees resigned prior to ER action, two employees were removed, three employees received a suspension of one day or more, seven employees received written reprimands or counseling, and one employee received no disciplinary action. A total of 27 cases referred by the OIG to ER are pending action at the end of the reporting period.

OIG Hotline Activity

The Investigations Division fielded 700 contacts through the internal OIG hotline. The OIG received 8,224 submissions on the external OIG hotline.



Significant Investigations

Senior Executive: Misuse of Government-owned Vehicles (GOVs)

An OIG investigation determined that a senior official misused GOVs and also borrowed funds from a subordinate on two occasions, totaling under $70.

The investigative findings were forwarded to the DoD OIG, ER, the Office of Personnel Security, and the subject's supervisor.

The case did not meet the requirements for reporting to DOJ.

GG15: Appearance of a Conflict of Interest

An OIG investigation determined that a former Agency employee created the appearance they were violating the law or ethical standards when they participated in matters potentially affecting contracts with a company for whom the employee's spouse was a manager.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

The case was reported to DOJ and not accepted for prosecution.

GG15: Restriction of Protected Disclosure to OIG

An OIG investigation determined that an Agency employee restricted and intimidated an individual from making a protected disclosure to the OIG; attempted to impede and influence an OIG investigation; and failed to promptly report to the OIG a reasonable belief of violation of law, rule, or regulation.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

The case did not meet the requirements for reporting to DOJ.

GG15: Abuse of Authority

An OIG investigation determined that a former Agency supervisor threatened to reprise against subordinates by not promoting them if they reported security violations to S&CI, requested that subordinates use official time to perform activities other than those required in the performance of their official duties, and failed to treat their subordinates with courtesy and respect.

The investigative findings were forwarded to ER and the Office of Personnel Security.

The case did not meet the requirements for reporting to DOJ.

GG15: Preferential Treatment

An OIG investigation determined an Agency supervisory employee, who was a part of a subordinate's formal promotion process, provided preferential treatment to that subordinate employee by reviewing portions of their promotion package and offering guidance in advance of their promotion submission.

The supervisor knew they would be reviewing the package as part of the formal promotion process and did not afford the same opportunities to any other subordinates.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

The case did not meet the requirements for reporting to DOJ.

GG14 and GG15: Whistleblower Reprisal

An OIG investigation determined that Agency supervisors did not reprise against a subordinate employee for making protected disclosures to management and the OIG, that there was no evidence of favoritism during the promotion process, and that the supervisors did not adversely affect the rights of the employee by abusing their authority.

The investigative findings were forwarded to DoD OIG.

Semiannual Reports on Investigations of Unauthorized Disclosures of Classified Information

In December 2019, the President of the United States signed into law the National Defense Authorization Act for Fiscal Year 2020 (NDAA). Section 6718 of the NDAA amends Title XI of the National Security Act of 1947 by adding a new section: "Section 1105 – Semiannual Reports on Investigations of Unauthorized Disclosures of Classified Information." This section requires the NSA OIG to submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information and do so not less frequently than once every six months.

During the period from 1 April through 30 September 2021, the OIG has not opened or completed any investigations of disclosures of information that has been determined to be classified.

Recoveries

During the reporting period, the OIG referred to the Agency proposed financial recoveries of approximately $752,687 based on substantiated fraud, and the Agency reported total actual recoveries of approximately $43,133 from prior referrals.

Summary of Additional Investigations

The NSA OIG opened 32 investigations and 83 inquiries while closing 42 investigations and 122 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, hostile work environment, violations of time and attendance, misuse of position, nepotism, false statements, and labor mischarging.

Contractor Labor Mischarging

The OIG opened four new contractor labor mischarging investigations and substantiated eight cases. The substantiated cases closed during the reporting period resulted in the proposed recoupment of approximately $681,688. Eleven investigations remain open.

Time and Attendance Fraud

The OIG opened six new investigations into employee time and attendance fraud and substantiated eight cases during the reporting period. The substantiated cases resulted in the proposed recoupment of approximately $67,575. Disciplinary action against eight employees for time and attendance fraud is pending with the Agency. Five investigations remain open.

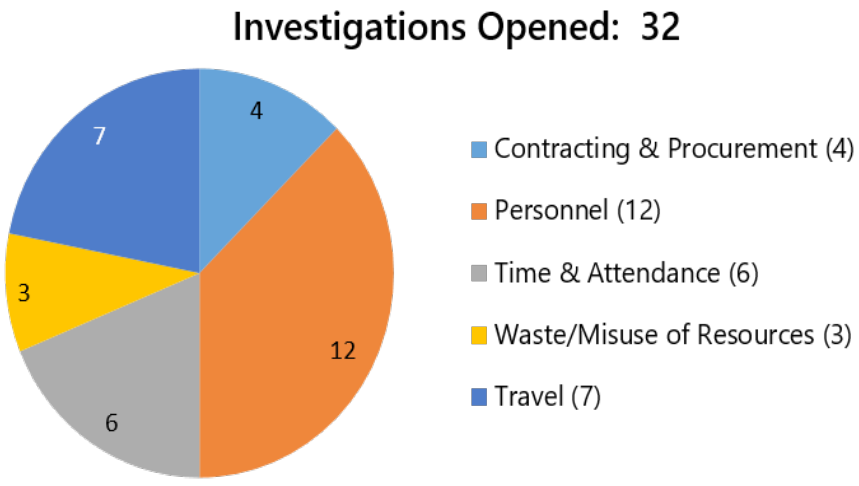
Computer Misuse

The OIG opened three new investigations involving allegations of computer misuse and substantiated two cases during the reporting period. Disciplinary action against one employee for computer misuse is pending with the Agency.

Investigations Summary

Total number of investigative reports issued	42
Total number of persons reported to DOJ for criminal prosecution	18
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments	0
Data contained in this report and table were obtained from the OIG Electronic Information Data Management System (eIDMS)	

Investigations Opened



Peer Review

System Review Report on the National Security Agency Office of Inspector General Audits Organization

The IC OIGs led a review of the NSA OIG Audits Division. The review team included representatives of the National Reconnaissance Office (NRO), Defense Intelligence Agency (DIA), and IC IGs and covered the three-year period that ended on 31 March 2021. The peer review determined that the system of quality control for the audits organization of the NSA OIG in effect for the year that ended 31 March 2021 has been suitably designed and complied with to provide the NSA OIG with reasonable assurance of performing and reporting in conformity with all applicable professional standards and applicable legal and regulatory requirements in all material respects. The peer review team also provided a letter of comment containing three findings that were not considered to be of sufficient significance to affect the opinion expressed in the peer review report, with recommendations to address each. The OIG concurred in all three recommendations and is taking action to address them.

External Peer Review of the Central Intelligence Agency, Office of the Inspector General, Office of Inspections

The NSA OIG led a peer review of the Central Intelligence Agency (CIA) OIG Inspections Division from 21 through 23 June 2021. The review team included representatives from DIA, NRO, and IC OIGs; the review covered the three-year period from FY 2018 through FY 2020. The peer review team assessed that the CIA OIG Inspections Division's policies and procedures were generally consistent with the seven Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards reviewed: quality control, planning, data collection and analysis, evidence, records maintenance, reporting, and follow-up. The team also assessed that all five of the reports reviewed generally complied with the required CIGIE standards.

Diversity and Engagement

Established in February 2018, the OIG Diversity and Engagement Committee's (DEC) mission is "to develop and maintain a culture that promotes and exemplifies the values of embracing diversity and the inclusion of varying thoughts, cultures, and experiences throughout the OIG, by offering a range of opportunities that foster professional growth and increase awareness of self and others."

Since its creation, the DEC's membership has grown significantly, as has its impact on the OIG workforce. Past successes include hosting two annual Diversity Days in 2019 and 2020; actively participating in CIGIE's DEI Working Groups; and hosting informative and educational Brown Bag sessions for the OIG workforce, including "Stress and Anxiety during COVID" and "Sadness, Grief, and Loss during COVID."

A significant highlight from the current reporting period was the DEC's week-long virtual diversity event for OIG staff and management, focused on professional development and expanding diversity, equity, inclusion, civility, and mental health awareness. We opened Diversity Week by unveiling the newly implemented OIG Mentoring Program, a DEC initiative, which will provide OIG personnel with mentoring opportunities in their skill community and encourage cross-OIG engagement. Other Diversity Week sessions included: "Everyday Diversity Practices," "Workplace Civility," "Transgender Awareness," "Suicide Awareness," "Post-Traumatic Stress Disorder Awareness," "Change and Change Agents at NSA: The African American Experience," and "NSA OIG: Realizing What Our Mirror Reveals." A "Cultural Connection through Food" event was icing on the cake. In a COVID-safe manner, the OIG workforce contributed foods, with descriptions of their cultural significance to their respective donors, for all to enjoy. This seemingly simple gesture of sharing food was a great way to bring the office together with a shared emphasis on the diversity that makes for a rich and strong workplace. We closed Diversity Week by announcing a new OIG honorary award, named in the memory of former IG Ralph W. Adams, Jr., who was the first and only African American to be IG at NSA. The award, the result of another DEC initiative, formally recognizes innovative, forward-thinking NSA OIG employees who, through their efforts, demonstrate and promote the advancement of DEI&A in the OIG.

Whistleblower Coordinator Program

The OIG has made whistleblower protection a priority. Whistleblowers perform an important service to NSA and the public when they come forward with what they reasonably believe to be evidence of wrongdoing. They should never suffer retaliation or reprisal for doing so. We consider whistleblowers to be a vital source of information that helps the OIG accomplish its mission by providing information that is critical to our ability to detect and deter waste, fraud, abuse, and misconduct throughout this extensive Agency and related to its diverse programs and operations.

The OIG operates a Hotline, staffed by experienced and knowledgeable investigators, to receive and process complaints from inside and outside of the Agency. Individuals may submit complaints anonymously; if the complainant elects to identify themselves, the OIG will maintain their confidentiality unless the complainant consents or disclosure is unavoidable. The OIG's Investigations Division examines all credible claims of reprisal.

Given the importance of whistleblowers to the Agency and the OIG, the OIG has taken steps to help ensure that Agency employees and others are fully informed about whistleblower rights and protections. To that end, the OIG worked with the Agency to develop an online whistleblower training, which DIRNSA has made mandatory for all NSA employees, and we continue to work with the Agency to refine the program based on user feedback and otherwise. Furthermore, the OIG's Whistleblower Coordinator serves as a resource by which Agency employees and others can obtain further information about their rights and protections. Finally, the OIG continues to work with Congress and other IC entities on legislative initiatives that would afford additional whistleblower protections.

This page intentionally left blank.

Appendix A: Audits, Inspections, Evaluations, and Oversight Memoranda Completed in the Reporting Period

Intelligence Oversight

Limited Scope Evaluation of NSA's Rules Based Targeting (RBT) Controls

Limited Scope Evaluation of United States Person (USP) Identifiers Used to Query against FISA Section 702 Data

Inspections

Enterprise Inspections

Inspection of the NSA/CSS Representative and Cryptologic Services Group to U.S. European Command

Inspection of the NSA/CSS Representative and Cryptologic Services Group to U.S. Africa Command

Quick Reaction Report on Concerns Discovered during an Inspection of the Cryptologic Services Group Key West

Short-Notice Inspection of NSA/CSS Representative to Defense Information Systems Agency/Joint Force Headquarters—Department of Defense Information Network

Joint Inspection of an Overseas Site

Advisory Memorandums

Cyberspace Workforce Improvement Program—Advisory Memorandum

Other Reports

Trends Noted in OIG Inspections August 2014-December 2020

External Peer Review of the Central Intelligence Agency, Office of the Inspector General, Office of Inspections

Audits

Mission and Mission Support Branch

Audit of NSA's Fiscal Year 2020 Compliance with the Payment Integrity Information Act of 2019

Audit of the Agency's Parking and Transportation Initiatives

Audit of the Agency's Management of Fit-up Costs

Audit of Cost-Reimbursement Contracts

Audit of the Allocation of Shared Expenses

Evaluation of NSA's FY2020 Application of Classification Markers, Compliance With Declassification Procedures, and the Effectiveness of Declassification Review Processes

Congressionally Required Audit on NSA's Security & Counterintelligence

Audit of Tactical Serialized Reporting

Cybersecurity and Technology Branch

Evaluation of the NSA Information Security Continuous Monitoring Program

Audit of Network Enclaves with Distributed Monitoring Oversight

Financial Audits Branch

Appropriations for Radome Purchases and Installations, Quick Reaction Report

FY2021 Statement of Standards for Attestation Engagement 18, NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

Appendix B: Audit Reports with Questioned Costs and Funds That Could Be Put to Better Use

Audit Reports with Questioned Costs[1]

Report	No. of Reports	Questioned Costs (including Unsupported Costs)	Unsupported Costs
For which no management decision had been made by start of reporting period	2	$460,000,000	$420,000,000
Issued during reporting period	1	$227,226,000	$227,226,000
For which management decision was made during reporting period			
Costs disallowed	0	0	0
Costs not disallowed	1	$460,000,000	$420,000,000
For which no management decision was made by end of reporting period	2	$227,226,000	$227,226,000

Audit Reports with Funds that Could Be Put to Better Use[2]

Report	No. of Reports	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0

[1] Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

[2] Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

Appendix C: Recommendations Overview

Recommendations Summary

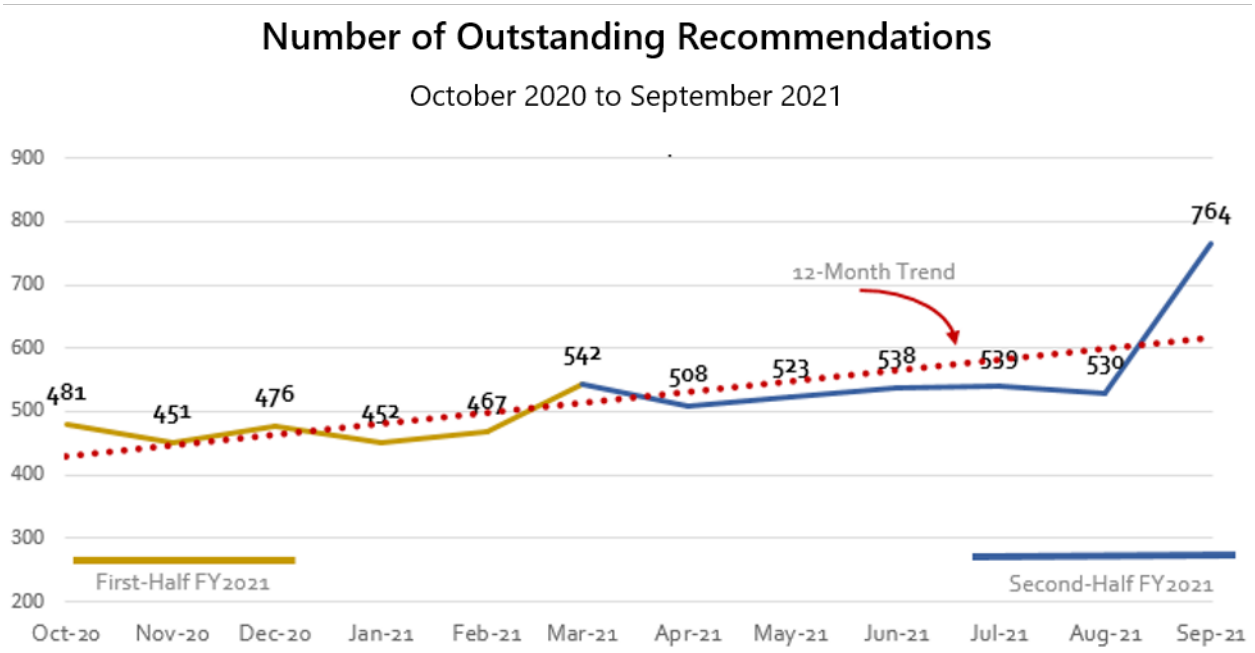
The OIG made 469 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 98 of the newly published recommendations and a total of 252 recommendations during the reporting period.

The OIG published 22 reports and other oversight products during this reporting period.

Outstanding Recommendations

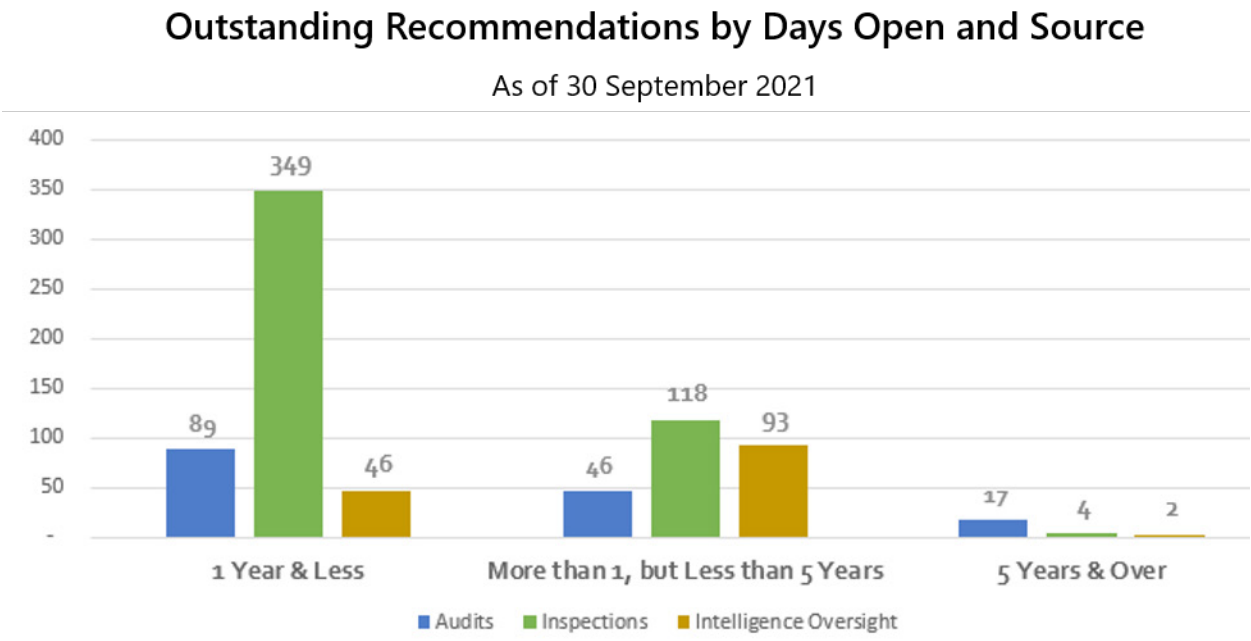
The OIG considers a report open when one or more recommendations contained in the report have not been closed. The number of outstanding recommendations is the total contained in all reports that remain outstanding.

	Audits	Inspections	Intelligence Oversight	Total
Open reports	38	40	23	101
Outstanding recommendations	152	471	141	764



Outstanding Recommendations Breakdown

Days Open Groupings	Audits	Inspections	Intelligence Oversight	Total
1 & Less	89	349	46	484
2-4 Years	46	118	93	257
5 & Over	17	4	2	23
Totals	**152**	**471**	**141**	**764**



Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and reviews detailed above, the OIG has issued 11 referrals to Agency management involving policy issues during the reporting period since August 2018. All 11 referrals were closed based upon Agency action prior to the reporting period.

Significant Outstanding Recommendations – Intelligence Oversight

Special Study of NSA Controls to Comply with FISA Section 702 Targeting and Minimization Procedures

The OIG conducted this study to determine whether select NSA controls are adequate to ensure compliance with FISA Section 702 targeting and minimization procedures. As part of this study, the OIG tested NSA's controls that ensure that data is queried in compliance with FISA Section 702 targeting and minimization procedures. The OIG found that NSA did not have a necessary system control. The Agency had previously identified this as a concern and has been working to implement a new system control. The OIG assessed that, until this system control is implemented, the Agency will be at risk for performing queries that do not comply with NSA's FISA Section 702 authority. The Agency has indicated that until the recommended system control is available, it has in place multiple processes to aid in ensuring query compliance. Nevertheless, the OIG believes that this recommendation, which has an original target completion date of December 2017, remains valid and significant for the Agency to address. The OIG understands that the Agency continues to work toward taking action to implement a pre-query compliance control by June 2022.

Joint Review of Overhead SIGINT Compliance at a Joint Facility

The NSA OIG conducted a joint review of overhead SIGINT compliance at a joint facility. The objectives of this joint review were to assess the application of SIGINT compliance policies and procedures; assess the processes or mechanisms for raising questions and resolving disagreements regarding programs or operations as they relate to SIGINT compliance; and identify any hurdles that may keep SIGINT compliance policies from keeping pace with technological advances in the overhead radio frequency (RF) collection environment.

The OIGs identified a number of hurdles that may hinder the application of SIGINT compliance policies and their ability to keep pace with technological advances in the overhead radio frequency environment. We also found that a process does not exist for raising questions and effectively resolving disagreements, and that there are no jointly accepted operating instructions for partner laboratory activities, which has resulted in what NSA at times has assessed to be noncompliant SIGINT access. As a result, the OIGs jointly made 18 recommendations, including 3 recommendations addressed directly to the Directors, to assist the Agencies in addressing the findings detailed in the report.

NSA and its partner agreed with all of the report's recommendations and agreed to take action sufficient to meet their intent. The agencies determined that the three recommendations to the Directors had to be resolved before the other recommendations could be addressed. The original target completion date for the three recommendations was March 2021. The OIGs have granted the Agencies two extensions, with current estimated completion date of March 2022 for two and June 2022 for the third, because the recommendations address complex issues that have proven challenging for the Agencies to resolve. The Agencies also anticipate a completion date of June 2022 for the recommendation that requires them to develop an escalation process for related disputes.

Significant Outstanding Recommendations – Inspections

Secure the Net / Secure the Enterprise / Insider Threat

Inspection teams find many instances of noncompliance with rules and regulations designed to protect computer networks, systems, and data. Significant outstanding inspection findings include:

- System Security Plans are often inaccurate and/or incomplete.
- Two-person access controls are not properly implemented for data centers and equipment rooms.
- Removable media are not properly scanned for viruses.

Continuity of Operations Planning

The OIG has noted Continuity of Operations program concerns across the last several years of inspections. The COVID-19 pandemic has reinforced these concerns. The OIG's *Evaluation of NSA's Mission Assurance/Continuity of Operations*, referenced in the Inspections section of this report, will evaluate the effectiveness and efficiency of this program and determine whether it meets all of the requirements of pertinent policies and regulations.

Emergency Management Plan

Many sites inspected do not have a mature, well-exercised Emergency Management Plan or Emergency Action Plan for the protection of personnel and the site. This encompasses situations such as an active shooter, natural disaster, and terrorist threat.

Assessment of NSA's Personnel Accountability Program

DoDI 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, issued 3 May 2010, establishes policy and assigns responsibilities for accounting and reporting of DoD-affiliated personnel following a natural or man-made disaster. Since CY 2011, DoDI 3001.02 has required IGs of DoD components to conduct evaluations biennially of the personnel accountability programs in their respective components to ensure compliance with this instruction.

As referenced under Inspections above, the OIG has begun a sixth biennial assessment to assess the Agency's compliance with the DoDI. The ability of the Agency to account for affiliated personnel is critical following a natural or man-made disaster, including events like the COVID-19 global pandemic. The lack of pre-planned guidance and procedures to account for all personnel could impact the ability to achieve prompt continuation of operations following an incident or in a similar situation in the future.

The DoD instruction requires the OIG to issue its report by February 2022.

Significant Outstanding Recommendations – Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

The OIG found in 2011 that Agency organizations and contractors are able to purchase information technology items without requisite approvals and recommended that the Agency implement automated compliance controls to address the issue. The Agency has implemented such a solution for software acquisitions and is developing and reviewing a process for hardware acquisitions.

The OIG also recommended that the Agency develop contract provisions to require contractors to comply with NSA/CSS Enterprise Solutions (NES)/Baseline Exception Request (BER) processes, as NSA/CSS Policy 6-1, *Management of NSA/CSS Global Enterprise IT Assets*, issued 8 September 2008, requires. This recommendation depends on implementation of the previous recommendation before mandatory contract provisions or language for hardware purchases and the processes can be developed and included in applicable contracts.

Audit of Removable Media

Removable media (RM) is any type of storage device (e.g., CDs, DVDs, USB drives) that can be removed from a computer while it is running. RM makes it easy for a Data Transfer Agent (DTA) to move data from one computer (or network) to another. The failure to manage and monitor the import or export of data using RM could result in the compromise of classified information or increase the risk of malware being transferred to critical networks. NSA asserts that it has implemented a combination of technical and administrative controls and is making improvements to the process, scheduled for review by 30 December 2021.

Joint Audit of Intragovernmental Transactions

Prior audits of NSA's financial statements determined that NSA was unable to substantiate the accuracy of transactions between the NSA and another agency, and this deficiency continues to contribute to a reported material weakness in the Agency's annual Report on Internal Control. Specifically, NSA has been unable to substantiate the accuracy of the amount its partner agency invoiced and liquidated against NSA advance payments or to demonstrate that NSA received the associated goods or services.

The OIGs recommended that the agencies establish and formally document an agreement on the reporting responsibilities of each agency and the allocation of joint program expenditures to each agency. In addition, the NSA OIG recommended that NSA implement procedures to ensure that the transactions associated with joint programs are recorded in accordance with U.S. generally accepted accounting principles. The OIGs for both agencies also recommended that each agency implement procedures for providing detailed and timely transaction-level documentation to the requesting agency to support expense activity on Economy Act Orders. Successful implementation of the recommendations will provide NSA increased assurance that it received what it paid for and improved accountability and financial reporting on its financial statements. All three of these recommendations are significant and outstanding as of the end of the reporting period.

Appendix D: Abbreviations List

ACC	Advanced Campaign Cell
ADA	Antideficiency Act
CARES	Coronavirus Aid, Relief, and Economic Security
CIA	Central Intelligence Agency
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CONUS	Continental U.S.
COR	Contracting Officer Representative
CRITIC	Critical information
CSG	Cryptologic Services Group
CWIP	Cyberspace Workforce Improvement Program
DCAA	Defense Contract Audit Agency
DEC	Diversity and Engagement Committee
DEI&A	Diversity, equity, inclusion, and accessibility
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIRNSA	Director, NSA
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDI	DoD Instruction
DOJ	Department of Justice
eIDMS	Electronic Information Data Management System
EO	Executive Order
ER	Employee Relations
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISMA	Federal Information Security Modernization Act
GOVs	Government-owned Vehicles
I&L	Installations & Logistics
IA/CYBER	Information assurance and cyberspace
IC	Intelligence Community
ICIG	Intelligence Community Inspector General
IG	Inspector General
IO	Intelligence oversight

ISCM	Information Security Continuous Monitoring
ITP	Insider Threat Program
MCT	Mission Correlation Table
NCR	NSA/CSS Representative
NCR AFRICOM	NCR and CSG Group to U.S. Africa Command
NCR DISA	NCR to DISA/Deputy NCR, U.S. Cyber Command for Joint Force Headquarters-Department of Defense Information Network
NCR EUCOM	NCR and CSG Group to U.S. European Command
NDAA	National Defense Authorization Act
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally identifiable information
PIIA	Payment Integrity Information Act
QRR	Quick Reaction Report
RBT	Rules-Based Targeting
RF	Radio frequency
RM	Removable media
S&CI	Security & Counterintelligence
SIGINT	Signals intelligence
TGRAM	Tactical serialized report
TTO	Technical Task Order
USP	United States person

Appendix E: Index of Reporting Requirements*

IG Act Reference	Reporting Requirements	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1–4
§5(a)(2)	Recommendations for corrective action	N/A
§5(a)(3)	Significant outstanding recommendations	32-34
§5(a)(4)	Matters referred to prosecutorial authorities	19
§5(a)(5)	Information or assistance refused	ii
§5(a)(6)	List of audit, inspection, and evaluation reports	27-28
§5(a)(7)	Summary of particularly significant reports	1–4
§5(a)(8)	Audit reports with questioned costs	29
§5(a)(9)	Audit reports with funds that could be put to better use	29
§5(a)(10)	Summary of reports for which no management decision was made	4
§5(a)(11)	Significant revised management decisions	4
§5(a)(12)	Significant management decision disagreements	4
§5(a)(13)	Information described under 05(b) of FFMIA of 1996	N/A
§5(a)(14)	Results of peer review conducted of NSA OIG	23
§5(a)(15)	List of outstanding recommendations from peer review of NSA OIG	N/A
§5(a)(16)	List of peer reviews and outstanding recommendations conducted by NSA OIG	23
§5(a)(17)	Statistical tables of investigations	22
§5(a)(18)	Description of Metrics used in statistical tables of investigations	22
§5(a)(19)	Reports concerning investigations of Seniors	20
§5(a)(20)	Whistleblower Retaliation	21
§5(a)(21)	Agency interference with IG Independence	ii
§5(a)(22)	Disclosure to the public	N/A
§5(a)(note)	P.L. 110-181 §845, Final completed contract audit reports	N/A
§5(a)(note)	P.L. 103-355 (as amended), Outstanding recommWendations past 12 months	30-34
* Citations are to the Inspector General Act of 1978, as amended.		

OFFICE OF THE INSPECTOR GENERAL

Pursuant to the Inspector General Act of 1978, as amended, and in accordance with NSA/CSS Policy 1-60, the NSA/CSS Office of the Inspector General (OIG) conducts independent oversight that promotes Agency respect for constitutional rights, adherence to laws, rules, and regulations, and the wise use of public resources. Through investigations and reviews, we detect and deter waste, fraud, abuse, and misconduct and promote the economy, the efficiency, and the effectiveness of Agency operations.

AUDIT

The Audit Division comprises three branches: Cybersecurity and Technology, Financial Audits, and Mission and Mission Support. The Division's audits and evaluations examine the economy, the efficiency, and the effectiveness of NSA programs and operations; assess Agency compliance with laws, policies, and regulations; review the operation of internal information technology and controls; and determine whether the Agency's financial statements and other fiscal reporting are fairly and accurately presented. Audits are conducted in accordance with auditing standards established by the Comptroller General of the United States.

INSPECTIONS

The Inspections Division performs organizational inspections and functional evaluations to assess adherence to regulations and policies and to promote the effective, efficient, and economical management of an organization, site, or function. OIG inspection reports recommend improvements and identify best practices across a broad range of topics, to include mission operations, security, facilities, and information technology systems. The Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other Intelligence Community (IC) entities to jointly inspect consolidated cryptologic facilities. Inspections and evaluations are conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) "Quality Standards for Inspection and Evaluation."

INTELLIGENCE OVERSIGHT

The Intelligence Oversight (IO) Division conducts evaluations that examine a wide range of NSA intelligence and intelligence-related programs and activities to assess if they are conducted efficiently and effectively, and are in compliance with federal law, executive orders and directives, and IC, DoD, and NSA policies, and appropriately protect civil liberties and individual privacy. The IO function is grounded in Executive Order 12333, which establishes broad principles for IC activities. IO evaluations are conducted in accordance with the CIGIE "Quality Standards for Inspection and Evaluation."

INVESTIGATIONS

The Investigations Division examines allegations of waste, fraud, abuse, and misconduct by NSA affiliates or involving NSA programs or operations. The investigations are based on submissions made through the classified or unclassified OIG Hotline, as well as information uncovered during OIG audits, inspections, and evaluations, and referrals from other internal and external entities. Investigations are conducted in accordance with the CIGIE "Quality Standards for Investigations."

How to Reach Us

9800 Savage Road, Suite 6247

Fort George G. Meade, Maryland 20755

HOTLINE

301.688.6327

FAX: 443.479.0099